IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF	)	
INFORMATION ASSOCIATED WITH	)	
STEVEN MICHAEL PURSELL	)	
FACEBOOK USER ID	)	
MICHAEL.PURSELL.01018,	)	Magistrate No. 17-377M
STORED AT PREMISES	)	[UNDER SEAL]
CONTROLLED BY FACEBOOK INC.	)	

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

I, Gregg Frankhouser, being duly sworn, depose and state:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook user ID that is stored at premises owned, maintained, controlled, or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the user ID. The account to be searched is under the name **STEVEN MICHAEL PURSELL** and has the associated **Facebook ID michael.pursell.01018** (hereinafter the "Target Account"). This account and the information to be searched is further described in the following paragraphs and in Attachment A.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), assigned to the Pittsburgh, Pennsylvania office. I have been employed as a Special Agent for the FBI since April 2002. As part of my duties, I investigate violations of federal law, including the online exploitation of children, including violations pertaining to the illegal possession, receipt, transmission, and production of material depicting the sexual exploitation of minors. I have gained

expertise in the conduct of such investigations through training in the area of child pornography and child exploitation investigations in seminars, classes, and everyday work related to conducting these types of investigations and have had the opportunity to observe and review numerous examples of child pornography in a variety of media, including computer media. I have obtained FBI Basic and Advanced Crimes Against Children Training. By virtue of my FBI employment, I perform and have performed a variety of investigative tasks, including the execution of federal search warrants and seizures, and the identification and collection of computer-related evidence. I have personally participated in the execution of numerous federal search warrants involving the search and seizure of computer equipment in cases involving violations of Sections 2250, 2251(a), 2252(a) and 2423—offenses involving the sexual exploitation of children and child pornography.

3. I know that Tile 18, United States Code, Section 2251(a) makes it a crime to produce material depicting the sexual exploitation of a minor (child pornography) and that Section 2252(a)(4)(B), makes it a crime to possess child pornography.

4. I also know that Title 18, United States Code, Section 2423(b) makes it a crime to travel for the purpose of engaging in illicit sexual conduct with a child. I am aware that the State of Pennsylvania criminalizes sexual contact with children, specifically with minors under 16 years of age.

5. As a federal agent, your affiant is authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

6. The statements in this affidavit are based in part on my investigation of this matter, including my personal observations, my training, and experience, and on information provided by other law enforcement agents. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this

investigation. I set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of a violations of Title 18, United States Code, Sections 2251(a), 2252(a)(4)(b), and 2423(b), is located within the Target Account.

7. In summary, the following affidavit sets forth facts establishing that **STEVEN MICHAEL PURSELL** traveled from West Virginia to meet with and have sexual contact with a fourteen-year-old female (Minor A) and recorded/archived/transmitted visual depictions and/or video via Facebook from his cellular telephone. Minor A told law enforcement that she met PURSELL via Facebook and that she communicated with him using Facebook messenger and video calls. Minor A's Facebook User ID is 100012633963829. On March 20, 2017, PURSELL arranged to meet Minor A via Facebook. Sometime before midnight that same day, PURSELL picked Minor A up near her home in Hookstown, Pennsylvania and transported her to a hotel in the Moon Township area of Western Pennsylvania where he sexually exploited her. Minor A reported that PURSELL set up his phone in a manner such that he could video record the sexual conduct and Minor A described this video as "live stream." Minor A stated that, on multiple occasions during the sexual contact, PURSELL would hold or position his cellular telephone in a way so as to record/archive/transmit depictions and/or video of Minor A engaged in sexually exploitative conduct with PURSELL. As set forth below, there is probable cause to believe that PURSELL used his Facebook account, specifically described hereto in "Attachment A," to facilitate the crime of traveling within interstate commerce to engage in criminal sexual activity with a minor. Additionally, there is probable cause to believe that PURSELL used his Facebook account ("Target Account") to record/archive/transmit visual depictions and/or video of his criminal sexual contact with Minor A.

8. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2251(a), 2252(a)(4)(B), and 2423(b) have been committed by STEVEN MICHAEL PURSELL and that evidence of these crimes may be found in the Target Account. Moreover, based upon the same, there is probable cause to believe that the Target Account contains evidence and/or instrumentalities of these crimes, as further described in Attachment B.

BACKGROUND REGARDING CHILD PORNOGRAPHY AND COMPUTERS

9. Based on your Affiant's training, experience, and knowledge, your Affiant knows the following:

a. Computers, computer technology, and cellular telephones have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers and mobile devices (e.g., smartphones, tablets) has added to the methods used by child pornography collectors/producers interact with and

sexually exploit children. Computers and mobile devices serve four functions in connection with child pornography; production, communication, distribution, and storage.

c. Child pornographers can now transfer photographs directly from a camera or mobile device to a computer storage system. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem, or via mobile devices. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer and Internet-capable mobile devices are preferred methods of distribution and receipt of child pornographic materials.

d. The advent of webcams and cellular phones with built-in cameras has enabled child pornographers to broadcast live transmissions of sexual abuse of minors by easily connecting the webcam or camera to the Internet. A webcam is a video camera that attaches to a computer or that is built into a laptop or desktop screen. The software included with webcams also permits an individual to capture and save live transmissions to the computer or peripheral storage devices. A webcam can be used in conjunction with an instant messaging service which permits real-time, direct, text-based communication between two or more people while permitting the individuals to view each other real-time via the webcam. However, a webcam is not required in order to receive live transmissions of activity that is taking place in front of another user's webcam. The same can be accomplished using a cellular telephone with a built-in camera. Such

cellular telephones can record still images or video, allowing the user to share the images and/or video in real time using direct, text-based communications between two people or more or, where the phone is also a "smart phone" with Internet access, a user can upload the images or videos taken with the phone's built-in camera to the Internet or a social media website.

e. The ability of a computer or mobile device to store images in digital form makes these devices an ideal repository for child pornography. A single floppy disk can store dozens of images and hundreds of pages of text, and CDs, DVDs, and flash drives can store hundreds of images and thousands of pages of text. The size of the electronic storage media (commonly referred to as the hard drive or thumb drive) used in home computers has grown tremendously within the last several years. Electronic storage devices with the capacity of 750 gigabytes are common, and electronic storage devices in excess of one terabyte (1,000 gigabytes) are now available for sale for low cost. These drives can store thousands of images at very high resolution. It is possible to use digital cameras and "video" cameras (designed primarily to record moving images), including those contained in mobile devices such as cellular telephones, to upload images to the Internet. Only through careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail generated by this activity.

f. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

g. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography in various formats, including services offered by Internet Portals such as Microsoft Live, Yahoo!, Google, and Dropbox, among others. The online services allow a user to set up an account with a remote computing service that provides email services as

well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer or electronic device such as a phone, tablet, or other device with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer and/or mobile devices, in most cases.

h. As is the case with most digital technology, communications by way of computer and mobile device can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files, cache, or ISP client software, among others). In addition to electronic communications, a computer or mobile device user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data. For example, computers often indefinitely retain archived conversations from instant messaging programs as well as messaging logs and files shared over instant messaging.

PROBABLE CAUSE

10. On or about March 24, 2017, Minor A's mother contacted Pennsylvania State Police (PSP) Trooper First Class (TFC) Joshua K. Thomas regarding her fourteen-year-old daughter, Minor A, having had sexual contact with a thirty-four-year-old male. Minor A's mother confronted her after being told by a friend of Minor A's that Minor A had met and had sexual intercourse with an adult. Minor A admitted to her mother that on March 20, 2017, sometime before midnight, she snuck out of her home at 129 Esther Drive, Hookstown, Pennsylvania to meet

an adult male who she had met on the Internet social media site Facebook approximately one month ago. The two then traveled to a Super 8 hotel in the Moon Township area of Allegheny County, Pennsylvania where they had unprotected sexual intercourse at the hotel. The adult then transported Minor A back to her residence at approximately 4:00 AM the next day.

11. TFC Thomas was able to determine that Minor A and the adult went to the Super 8 hotel located at 8991 University Boulevard, Coraopolis, PA 15108. Super 8 hotel employees confirmed that an adult male by the name of STEVEN MICHAEL PURSELL checked into the hotel shortly before midnight on March 20, 2017 and checked out shortly after 9:00 AM on March 21, 2017.

12. TFC Thomas obtained the following documentation from the Super 8 hotel in Coraopolis, PA with regard to room rented by PURSELL on March 20, 2017: (i) a registration form signed by STEVEN PURSELL, (ii) a photo copy of PURSELL'S West Virginia driver's license, (iii) PURSELL'S U.S. Department of Veteran's Affairs identification card, and PURSELL'S USAA Visa credit card. Super 8 hotel employees also provided footage from the hotel's video surveillance that shows PURSELL checking into the hotel and entering the lobby area of the hotel with Minor A on March 20, 2017.

13. On March 28, 2017, TFC Thomas interviewed Minor A at the PSP Beaver Barracks. During the interview, Minor A relayed the following: Minor A met PURSELL on the Internet social media site, Facebook, approximately one month prior to their physical meeting on March 20, 2017. They met when PURSELL sent Minor A a Facebook friend request. Thereafter, they used Facebook Messenger and video calling to communicate. Minor A accessed Facebook from the laptop that was supplied to her by her school. Minor A stated that she and PURSELL communicated exclusively on Facebook and almost every day. She stated that their conversations

routinely were sexual in nature. Specifically, they talked about Minor A and PURSELL having sex. Minor A informed PURSELL that she was fourteen years old. According to Minor A, when she told PURSELL that she was fourteen years old "it didn't faze him." On Monday, March 20, 2017, PURSELL made plans with Minor A to travel to Western Pennsylvania, pick Minor A up at her home, and take her to a hotel to have sex. Minor A gave PURSELL her home address and, that same day, PURSELL traveled from West Virginia to Western Pennsylvania and followed through with their plans—he picked Minor A up at an intersection near her home and transported her in his vehicle to the Super 8 hotel in Coraopolis, PA.

14. Minor A reported that PURSELL picked her up some time before midnight. Minor A confirmed that the person in the vehicle that picked her up was in fact the person with whom she had been communicating via Facebook over the previous month. She described the individual as a white male, heavy build, dark hair and a tattoo of "Chinese characters" on his forearm. While the two traveled to the hotel, PURSELL told Minor A: "I'm risking a lot for you." Upon arriving at the hotel, PURSELL told Minor A to remain in the vehicle while he went into the lobby of the hotel. After PURSELL returned to the vehicle, he directed Minor A to walk ahead of him into the hotel. This was confirmed by video provided by the hotel.

15. Minor A went with PURSELL into room 311 of the Super 8 hotel. Minor A related that upon entering the room, she went into the bathroom to change. PURCELL entered the bathroom while she was changing, and began kissing her. When PURSELL exited the bathroom, Minor A began to shave her legs and pubic area. PURSELL then reentered the bathroom and held his phone in such a way that Minor A believed PURSELL was video recording and/or taking photographs of Minor A shaving her legs and pubic area. When Minor A exited the bathroom, PURSELL picked her up and placed her on the bed where he pulled down the top of her dress,

exposing Minor A's breasts. She felt uncomfortable and pulled the dress back up over her chest. She stated that this happened multiple times. Ultimately, PURSELL placed his mouth on Minor A's bare breasts. PURSELL also performed oral sex on Minor A and had unprotected vaginal sex with her until he ejaculated inside her.

16. Minor A also described how PURSELL used men's neck ties to bind her. She described how the ties were placed around her head and across her mouth as a gag, and that this binding attached to another that bound her hands and feet. Minor A described the position as being "hog tied." While Minor A was bound, PURSELL touched her around her vaginal area and put his fingers inside of her vagina. PURSELL removed the bindings when Minor A told him that they hurt her. After PURSELL removed the bindings, he began manipulating his cell phone and then showed Minor A his cell phone screen, which was set to video mode. Minor A described the video as still running and stated that she saw a comment on PURSELL's cell phone screen from an unknown individual stating: "She doesn't look 18." Minor A described the video as a "live stream" and recalled seeing other comments on the screen. PURSELL then told her: "I made $5." PURSELL then set up his cell phone in a position such that it could record their sexual activity on the bed. While PURSELL's cell phone was set up in this manner, Minor A performed oral sex on PURSELL and PURSELL again had vaginal sex with Minor A to the point of ejaculation.

17. At approximately 4:00 AM, PURSELL drove Minor A home in his personal vehicle. PURSELL then told Minor A not to contact him anymore and subsequently blocked her on Facebook.

18. Considering all of the foregoing, probable cause exists that evidence related to PURSELL's violation of federal crimes involving child sexual exploitation will be found in the Target Account.

19. On March 27, 2017, TFC Thomas sent a preservation request to Facebook for PURSELL's Facebook account.

20. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

21. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

22. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

23. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook

users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

24. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

25. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

26. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on

Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

27. Facebook also has a feature called Facebook Live that allows users to share live video with their followers and friends on Facebook. After the broadcast of the Live video ends, the video is published on the user's Facebook page or profile so that the user's followers and friends may watch the video at a later time, similar to any other post.

28. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

29. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

30. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

31. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the

account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

32. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

33. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

34. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

35. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

36. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings;

rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

37. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

38. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

39. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution"

evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

40. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

41. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

42. Based on the foregoing, I request that the Court issue the proposed search warrant.

43. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

GREGG FRANKHOUSER
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before
me this 24th day of April, 2017

United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Facebook account held by **STEVEN MICHAEL PURSELL** and associated with **Facebook ID michael.pursell.01018** that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;

(d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes;

tags; and information about the user's access and use of any Facebook applications, including Facebook Live;

(e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

(f) All "check ins" and other location information;

(g) All IP logs, including all records of the IP addresses that logged into the account;

(h) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(i) All information about the Facebook pages that the account is or was a "fan" of;

(j) All past and present lists of friends created by the account;

(k) All records of Facebook searches performed by the account;

(l) All information about the user's access and use of Facebook Marketplace;

(m) The types of service utilized by the user;

(n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(p) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2251(a), 2252(a)(4)(B), and 2423(b) involving **STEVEN MICHAEL PURSELL** since February 1, 2017 including, for each user ID identified on Attachment A, information pertaining to the following matters:

(a) Any and all communications to and from **STEVEN MICHAEL PURSELL** associated with **Facebook ID michael.pursell.01018** and Minor A (Facebook User ID 100012633963829);

(b) Messages, correspondence, documents and records pertaining to the production, receipt, distribution, and/or possession of material depicting the sexual exploitation of minors, as well as information indicating the location of the account user and the identity of the account use.

(c) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;

(d) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;

(e) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(f) The identity of the person(s) who communicated with the Target Account about matters relating to the crimes under investigation;

(g) Any other evidence relevant to the possible violations of 18 U.S.C. §§ 2251(a), 2252(a)(4)(B), and 2423(b) being investigated in this matter.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Facebook, and my official title is _____. I am a custodian of records for Facebook. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Facebook, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Facebook; and

c. such records were made by Facebook as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature